

# A reduced fast construction of polynomial lattice point sets with low weighted star discrepancy

Ralph Kritzinger\*, Helene Laimer†, Mario Neumüller‡

## Abstract

The weighted star discrepancy is a quantitative measure for the performance of point sets in quasi-Monte Carlo algorithms for numerical integration. We consider polynomial lattice point sets, whose generating vectors can be obtained by a component-by-component construction to ensure a small weighted star discrepancy. Our aim is to significantly reduce the construction cost of such generating vectors by restricting the size of the set of polynomials from which we select the components of the vectors. To gain this reduction we exploit the fact that the weights of the spaces we consider decay very fast.

*Keywords:* weighted star discrepancy, polynomial lattice point sets, quasi-Monte Carlo integration, component-by-component algorithm

*MSC 2000:* 11K06, 11K38, 65D30, 65D32

## 1 Introduction

A convenient way to approximate the value of an integral

$$I_s(F) := \int_{[0,1]^s} F(\mathbf{x}) \, d\mathbf{x}$$

over the  $s$ -dimensional unit cube is to use a quasi-Monte Carlo rule of the form

$$Q_{N,s}(F) := \frac{1}{N} \sum_{n=0}^{N-1} F(\mathbf{x}_n). \quad (1)$$

The integrand  $F$  usually stems from some suitable (weighted) function space and the multiset  $\mathcal{P}$  of integration nodes  $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$  in the algorithm  $Q_{N,s}(F)$  is chosen deterministically from  $[0,1]^s$ . For comprehensive information on quasi-Monte Carlo algorithms consult, e.g., [5, 3, 9, 12]. The quality of a quasi-Monte Carlo rule is for instance measured by some notion of discrepancy. In this paper we consider the weighted star discrepancy, which has been introduced by Sloan and Woźniakowski in [21], exploiting the insight that the weights reflect the influence of different coordinates on the

---

\*R. Kritzinger is supported by the Austrian Science Fund (FWF): Project F5509-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

†H. Laimer is supported by the Austrian Science Fund (FWF): Project F5506-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

‡M. Neumüller is supported by the Austrian Science Fund (FWF): Project F5505-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

integration error. Let  $[s] := \{1, 2, \dots, s\}$  and consider a weight sequence  $\gamma = (\gamma_u)_{u \subseteq [s]}$  of nonnegative real numbers, i.e., every group of variables  $(x_i)_{i \in u}$  is equipped with a weight  $\gamma_u$ . Roughly speaking, a small weight indicates that the corresponding variables contribute little to the integration problem. For simplicity, throughout this paper we only consider product weights, defined as follows. Given a non-increasing sequence of positive real numbers  $(\gamma_j)_{j \geq 1}$  with  $\gamma_j \leq 1$  we set  $\gamma_u := \prod_{j \in u} \gamma_j$  and  $\gamma_\emptyset := 1$ .

**Definition 1** Let  $\gamma = (\gamma_u)_{u \subseteq [s]}$  be a weight sequence and  $\mathcal{P} = \{\mathbf{x}_0, \dots, \mathbf{x}_{N-1}\} \subseteq [0, 1]^s$  be an  $N$ -element point set. The local discrepancy of the point set  $\mathcal{P}$  at  $\mathbf{t} = (t_1, \dots, t_s) \in (0, 1]^s$  is defined as

$$\Delta(\mathbf{t}, \mathcal{P}) := \frac{1}{N} \sum_{n=0}^{N-1} \mathbf{1}_{[0, \mathbf{t})}(\mathbf{x}_n) - \prod_{j=1}^s t_j,$$

where  $\mathbf{1}_{[0, \mathbf{t})}$  denotes the characteristic function of  $[\mathbf{0}, \mathbf{t}) := [0, t_1) \times \dots \times [0, t_s)$ . The weighted star discrepancy of  $\mathcal{P}$  is then defined as

$$D_{N, \gamma}^*(\mathcal{P}) := \sup_{\mathbf{t} \in (0, 1]^s} \max_{\emptyset \neq u \subseteq [s]} \gamma_u |\Delta((\mathbf{t}_u, \mathbf{1}), \mathcal{P})|,$$

where  $(\mathbf{t}_u, \mathbf{1})$  denotes the vector  $(\tilde{t}_1, \dots, \tilde{t}_s)$  with  $\tilde{t}_j = t_j$  if  $j \in u$  and  $\tilde{t}_j = 1$  if  $j \notin u$ .

A relation between the integration error of quasi-Monte Carlo rules and the weighted star discrepancy is given by the Koksma-Hlawka type inequality (see [21])

$$|Q_{N, s}(F) - I_s(F)| \leq D_{N, \gamma}^*(\mathcal{P}) \|F\|_\gamma,$$

where  $\|\cdot\|_\gamma$  is some norm which depends only on the weight sequence  $\gamma$  but not on the point set  $\mathcal{P}$ .

It turns out that lattice point sets (see, e.g., [12, Chapter 5], [9]) and polynomial lattice point sets (see, e.g., [12, Chapter 4], [13], [5, Chapter 10]) are often a good choice as sample points in (1). These two kind of point sets are strongly connected and have a lot of parallel tracks in their analysis. However, there are some situations where one type of point set is superior to the other in terms of error bounds or the size of the function classes where they yield good results for numerical integration. Thus it is beneficial to have constructions for lattice point sets as well as for polynomial lattice point sets at hand. For a detailed comparison of lattice point sets and polynomial lattice point sets see, e.g., [19]. Also, Ch. Schwab, in response to the first author's talk about constructing lattice point sets at the MCQMC 2016 conference in Stanford, pointed out that it would be an interesting problem to extend the result in [7] to polynomial lattice point sets. Thus, in this paper we study polynomial lattice point sets, a special class of point sets with low weighted star discrepancy, introduced by Niederreiter in [12, Chapter 4], [13]. For a prime number  $p$ , let  $\mathbb{F}_p$  be the finite field of order  $p$ . We identify  $\mathbb{F}_p$  with the set  $\{0, 1, \dots, p-1\}$  equipped with the modulo  $p$  arithmetic. We denote by  $\mathbb{F}_p[x]$  the set of polynomials over  $\mathbb{F}_p$  and by  $\mathbb{F}_p((x^{-1}))$  the field of formal Laurent series over  $\mathbb{F}_p$  with elements of the form

$$L = \sum_{l=\omega}^{\infty} t_l x^{-l},$$

where  $\omega \in \mathbb{Z}$  and  $t_l \in \mathbb{F}_p$  for all  $l \geq \omega$ . For a given dimension  $s \geq 2$  and some integer  $m \geq 1$  we choose a so-called modulus  $f \in \mathbb{F}_p[x]$  with  $\deg(f) = m$  as well as polynomials

$g_1, \dots, g_s \in \mathbb{F}_p[x]$ . The vector  $\mathbf{g} = (g_1, \dots, g_s)$  is called the generating vector of the polynomial lattice point set. Further, we introduce the map  $\phi_m : \mathbb{F}_p((x^{-1})) \rightarrow [0, 1)$  such that

$$\phi_m \left( \sum_{l=\omega}^{\infty} t_l x^{-l} \right) = \sum_{l=\max\{1, \omega\}}^m t_l p^{-l}.$$

With  $n \in \{0, 1, \dots, p^m - 1\}$  we associate the polynomial

$$n(x) = \sum_{r=0}^{m-1} n_r x^r \in \mathbb{F}_p[x],$$

as each such  $n$  can uniquely be written as  $n = n_0 + n_1 p + \dots + n_{m-1} p^{m-1}$  with digits  $n_r \in \{0, 1, \dots, p-1\}$  for all  $r \in \{0, 1, \dots, m-1\}$ . With this notation, the polynomial lattice point set  $\mathcal{P}(\mathbf{g}, f)$  is defined as the set of  $N := p^m$  points

$$\mathbf{x}_n = \left( \phi_m \left( \frac{n(x)g_1(x)}{f(x)} \right), \dots, \phi_m \left( \frac{n(x)g_s(x)}{f(x)} \right) \right) \in [0, 1)^s$$

for  $0 \leq n \leq p^m - 1$ . See also [5, Chapter 10].

In the following, by  $G_{p,m}$  we denote the set of all polynomials  $g$  over  $\mathbb{F}_p$  with  $\deg(g) < m$ . Further we define

$$G_{p,m}(f) := \{g \in G_{p,m} \mid \gcd(g, f) = 1\}. \quad (2)$$

For the weighted star discrepancy of a polynomial lattice point set we simply write  $D_{N,\gamma}^*(\mathbf{g}, f)$ .

Niederreiter [12] proved the existence of polynomial lattice point sets with low unweighted star discrepancy by averaging arguments. Generating vectors of good polynomial lattice point sets can be constructed by a component-by-component (CBC) construction. The standard structure of CBC constructions is as follows. We start by setting the first coordinate of the generating vector equal to 1. After this first step we proceed by increasing the dimension of the generating vector by one in each step until we have a generating vector  $(g_1, \dots, g_s)$  of full size  $s$ . That is, all previously chosen components stay the same and one new component is added. This new coordinate is chosen from a given search set, most commonly from  $G_{p,m}(f)$  given by (2). Usually it is determined such that the weighted star discrepancy of the lattice point set, corresponding to the generating vector, consisting of all previously chosen components plus one additional component, is minimized as a function of this last component.

Such constructions were provided in [4] for an irreducible modulus  $f$  and in [1] for a reducible  $f$ . In these papers, the authors considered the unweighted star discrepancy as well as its weighted version, which we study here. It is the aim of the present paper to speed up these constructions by reducing the search sets for the components of the generating vector  $\mathbf{g}$  according to each component's importance. It is the nature of product weighted spaces that the components  $g_j$  of the generating vector have less and less influence on the quality of the corresponding polynomial lattice point as  $j$  increases. Roughly speaking this is due to the weights  $(\gamma_j)$  that are becoming ever smaller with increasing index  $j$ . We want to exploit this property in the following way. As the components' influence is decreasing with their indices we want to use less and less time and computational cost to choose these components. To achieve this we choose them

from smaller and smaller search sets, which are defined as follows. Let  $w_1 \leq w_2 \leq \dots$  be a non-decreasing sequence of nonnegative integers. This sequence of  $w_j$ 's is determined in accordance with the weight sequence  $\gamma$ . Loosely speaking, the smaller  $\gamma_j$ , the bigger  $w_j$  is chosen. For  $w \in \mathbb{N}_0$  with  $w < m$  we define  $G_{p,m-w}$  and  $G_{p,m-w}(f)$  analogously to  $G_{p,m}$  and  $G_{p,m}(f)$ , respectively. Further we set

$$\mathcal{G}_{p,m-w}(f) := \begin{cases} G_{p,m-w}(f) & \text{if } w < m, \\ \{1 \in \mathbb{F}_p[x]\} & \text{if } w \geq m \end{cases}$$

for any  $w \in \mathbb{N}_0$ . For  $w < m$  these sets have cardinality  $p^{m-w} - 1$  in the case of an irreducible modulus  $f$  and  $p^{m-w-1}(p-1)$  for the special case  $f : \mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto x^m$ . We will consider these two cases in what follows. Finally, for  $d \in [s]$ , we define  $\mathcal{G}_{p,m-w}^d(f) := \mathcal{G}_{p,m-w_1}(f) \times \dots \times \mathcal{G}_{p,m-w_d}(f)$ . The idea is to choose the  $i$ th component of  $\mathbf{g}$  of the form  $x^{w_i} g_i$ , where  $g_i \in \mathcal{G}_{p,m-w_i}(f)$ , i.e., the search set for the  $i$ th component is reduced by a factor  $p^{-\min\{w_i, m\}}$  in comparison to the standard CBC construction. We will show that under certain conditions on the weights  $\gamma$  and the parameters  $w_i$  a polynomial lattice point set constructed according to our reduced CBC construction has a low weighted star discrepancy of order  $N^{-1+\delta}$  for all  $\delta > 0$ . The standard CBC construction (cf. [20]) can be done in  $\mathcal{O}(sN^2)$  operations. To speed up the construction, in a first step, making use of ideas from Nuyens and Cools [17, 18] on fast Fourier transformation, the construction cost can be reduced to  $\mathcal{O}(sN \log N)$ , as for example done in [4]. Combining this with our reduced search sets we obtain a computational cost that is independent of the dimension eventually. Reduced CBC constructions have been introduced first by Dick et al. in [2] for lattice and polynomial lattice point sets with a small worst case integration error in Korobov and Walsh spaces, respectively, and have also been investigated in [7] for lattice point sets with small weighted star discrepancy.

An interesting aspect of the discrepancy of high dimensional point sets is the so-called tractability of discrepancy (see, e.g., [14, 15, 16] for detailed information). For  $N, s \in \mathbb{N}$  let

$$\text{disc}_\infty(N, s) := \inf_{\substack{\mathcal{P} \subseteq [0,1]^s \\ \#\mathcal{P}=N}} D_{N,\gamma}^*(\mathcal{P}),$$

the  $N$ th minimal star discrepancy. To introduce the concept of tractability of discrepancy we define the information complexity (also called the inverse of the weighted star discrepancy) as

$$N^*(s, \varepsilon) := \min\{N \in \mathbb{N} \mid \text{disc}_\infty(N, s) \leq \varepsilon\}.$$

Thus  $N^*(s, \varepsilon)$  is the minimal number of points required to achieve a weighted star discrepancy of at most  $\varepsilon$ . To keep the construction cost of our generating vector low, it is, of course, beneficial to have a small information complexity and thus to stand a chance to have a polynomial lattice point set of small size. This is why we are interested in how fast the information complexity grows when  $s$  and  $\varepsilon^{-1}$  tend to infinity. Tractability describes this dependence of the information complexity on the dimension  $s$  and the error demand  $\varepsilon$ . The best we can hope for is the case where  $N^*(s, \varepsilon)$  is independent of  $s$  and depends at most polynomially on  $\varepsilon^{-1}$ . To be more precise, we say that we achieve strong polynomial tractability if there exist constants  $C, \tau > 0$  such that

$$N^*(s, \varepsilon) \leq C\varepsilon^{-\tau}$$

for all  $s \in \mathbb{N}$  and all  $\varepsilon \in (0, 1)$ . Roughly speaking, a problem is considered tractable if its information complexity's dependence on  $s$  and  $\varepsilon^{-1}$  is not exponential. Taking weights into account in the definition of discrepancy can sometimes overcome the so-called curse of dimensionality, i.e., an exponential dependence of  $N^*(s, \varepsilon)$  on  $s$ . We will show that our reduced fast CBC algorithm finds a generating vector  $\mathbf{g}$  of a polynomial lattice point set that achieves strong polynomial tractability provided that

$$\sum_{j=1}^{\infty} \gamma_j p^{w_j} < \infty$$

with a construction cost of

$$\mathcal{O} \left( N + \min\{s, t\}N + N \sum_{d=1}^{\min\{s, t\}} (m - w_d) p^{-w_d} \right)$$

operations, where  $t = \max\{j \in \mathbb{N} \mid w_j < m\}$ .

Before stating our main results we would like to discuss a motivating example. Consider first the standard CBC construction as treated in [1, 4], where  $w_j = 0$  for all  $j \geq 0$ . In this case, a sufficient condition for strong polynomial tractability is  $\sum_{j=1}^{\infty} \gamma_j < \infty$ , which for instance is satisfied for the special choices  $\gamma_j = j^{-2}$  and  $\gamma_j = j^{-1000}$ . However, in the second example the weights decay much faster than in the first. We can make use of this fact by introducing the sequence  $\mathbf{w} = (w_j)_{j \geq 0}$  such that the condition  $\sum_{j=1}^{\infty} \gamma_j p^{w_j} < \infty$  holds, while still achieving strong polynomial tractability (see Corollary 2). This way, we can reduce the size of the search sets for the components of the generating vector if the weights  $\gamma_j$  decay very fast. Consider for example the weight sequence  $\gamma_j = j^{-k}$  for some  $k > 1$ . For  $w_j = \lfloor (k - \alpha) \log_p j \rfloor$  with arbitrary  $1 < \alpha < k$  we find

$$\sum_{j=1}^{\infty} \gamma_j p^{w_j} \leq \sum_{j=1}^{\infty} j^{-k} j^{k-\alpha} = \sum_{j=1}^{\infty} j^{-\alpha} = \zeta(\alpha) < \infty,$$

where  $\zeta$  denotes the Riemann Zeta function. Observe that for large  $k$ , i.e., fast decaying weights, we may choose smaller search sets and thereby speed up the CBC algorithm.

This paper is organized as follows. In the next section we give an algorithm for constructing polynomial lattice point sets and we derive an upper bound on the weighted star discrepancy of the point set constructed with this algorithm. We also give tractability results and analyze the computational cost of our algorithm. At first, we consider the case where  $f : \mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto x^m$ . Then we consider the case where the modulus of the polynomial lattice point set is irreducible.

## 2 A reduced CBC construction

In this section we present a CBC construction for the vector  $(x^{w_1} g_1, \dots, x^{w_s} g_s)$  and an upper bound for the weighted star discrepancy of the corresponding polynomial lattice point set.

First note that if  $\mathbf{g} \in G_{p,m}^s$ , then it is known (see [4]) that

$$D_{N,\gamma}^*(\mathbf{g}, f) \leq \sum_{\substack{\mathbf{u} \subseteq [s] \\ \mathbf{u} \neq \emptyset}} \gamma_{\mathbf{u}} \left( 1 - \left( 1 - \frac{1}{N} \right)^{|\mathbf{u}|} \right) + R_{\gamma}^s(\mathbf{g}, f), \quad (3)$$

where in the case of product weights we have

$$R_\gamma^s(\mathbf{g}, f) = \sum_{\substack{\mathbf{h} \in G_{p,m}^s \setminus \{\mathbf{0}\} \\ \mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}}} \prod_{i=1}^s r_p(h_i, \gamma_i). \quad (4)$$

Here, for elements  $\mathbf{h} = (h_1, \dots, h_s)$  and  $\mathbf{g} = (g_1, \dots, g_s)$  in  $G_{p,m}^s$  we define the scalar product by  $\mathbf{h} \cdot \mathbf{g} := h_1 g_1 + \dots + h_s g_s$ . The numbers  $r_p(h, \gamma)$  for  $h \in G_{p,m}$  and  $\gamma \in \mathbb{R}$  are defined as

$$r_p(h, \gamma) = \begin{cases} 1 + \gamma & \text{if } h = 0, \\ \gamma r_p(h) & \text{otherwise,} \end{cases}$$

where for  $h = h_0 + h_1 x + \dots + h_a x^a$  with  $h_a \neq 0$  we set

$$r_p(h) = \frac{1}{p^{a+1} \sin^2\left(\frac{\pi}{p} h_a\right)}.$$

Thus, in order to analyze the weighted star discrepancy of a polynomial lattice point set it suffices to investigate the quantity  $R_\gamma^s(\mathbf{g}, f)$ . This is due to the result of Joe [10], who proved that for any summable weight sequence  $(\gamma_j)_{j \geq 1}$  we have

$$\sum_{\substack{\mathbf{u} \subseteq [s] \\ \mathbf{u} \neq \emptyset}} \gamma_{\mathbf{u}} \left( 1 - \left( 1 - \frac{1}{N} \right)^{|\mathbf{u}|} \right) \leq \frac{\max(1, \Gamma) e^{\sum_{i=1}^{\infty} \gamma_i}}{N},$$

with  $\Gamma := \sum_{i=1}^{\infty} \frac{\gamma_i}{1 + \gamma_i}$ .

**Algorithm 1** Let  $p \in \mathbb{P}$ ,  $m \in \mathbb{N}$ ,  $f \in \mathbb{F}_p[x]$  and let  $(w_j)_{j \geq 1}$  be a non-decreasing sequence of nonnegative integers and consider product weights  $(\gamma_j)_{j \geq 1}$ . Construct  $(g_1, \dots, g_s) \in \mathcal{G}_{p,m-\mathbf{w}}^s(f)$  as follows:

1. Set  $g_1 = 1$ .
2. For  $d \in [s-1]$  assume  $(g_1, \dots, g_d) \in \mathcal{G}_{p,m-\mathbf{w}}^d(f)$  to be already found. Choose  $g_{d+1} \in \mathcal{G}_{p,m-w_{d+1}}(f)$  such that

$$R_\gamma^{d+1}(x^{w_1} g_1, \dots, x^{w_d} g_d, x^{w_{d+1}} g_{d+1})$$

is minimized as a function of  $g_{d+1}$ .

3. Increase  $d$  by 1 and repeat the second step until  $(g_1, \dots, g_s)$  is found.

**Remark 1** Of course we have  $\mathcal{G}_{p,m-\mathbf{w}}^s(f) \subseteq G_{p,m}^s$ , and thus in Algorithm 1 it indeed suffices to consider  $R_\gamma^{d+1}$  rather than the weighted star discrepancy.

In the algorithm above, the search set is reduced for each coordinate of  $(g_1, \dots, g_s)$  according to its importance, as with increasing  $w_j$  the search set becomes smaller, as the weight  $\gamma_j$  and thus the corresponding component's influence on the quality of the generating vector decreases. For this reason we call Algorithm 1 a reduced CBC algorithm. We will now study Algorithm 1 for different choices of  $f$ .

## 2.1 Polynomial lattice point sets for $f(x) = x^m$

We will now study the interesting case where  $f: \mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto x^m$ . Throughout the rest of this section we write  $x^m$  instead of  $f$  to emphasize our special choice of  $f$ . Note that for  $g \in \mathbb{F}_p((x^{-1}))$  the Laurent series  $g/f$  can be easily computed in this case by shifting the coefficients of  $g$   $m$  times to the left. It is the aim of this section to prove the following theorem:

**Theorem 1** *Let  $\gamma = (\gamma_j)_{j \geq 1}$  and  $\mathbf{w}$  with  $0 = w_1 \leq w_2 \leq \dots$ . Let further  $(g_1, \dots, g_s) \in \mathcal{G}_{p, m-\mathbf{w}}^s(x^m)$  be constructed using Algorithm 1. Then we have for every  $d \in [s]$*

$$R_{\gamma}^d((x^{w_1}g_1, \dots, x^{w_d}g_d), x^m) \leq \frac{1}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right).$$

As a direct consequence we obtain the following discrepancy estimate.

**Corollary 1** *Let  $N = p^m$  and  $\gamma, \mathbf{w}$  and  $(g_1, \dots, g_s)$  as in Theorem 1. Then the polynomial lattice point set  $\mathcal{P}((x^{w_1}g_1, \dots, x^{w_s}g_s), x^m)$  has a weighted star discrepancy*

$$\begin{aligned} D_{N, \gamma}^*((x^{w_1}g_1, \dots, x^{w_s}g_s), x^m) \\ \leq \sum_{\substack{u \subseteq [s] \\ u \neq \emptyset}} \gamma_u \left( 1 - \left( 1 - \frac{1}{N} \right)^{|u|} \right) + \frac{1}{N} \prod_{i=1}^s \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right). \end{aligned} \quad (5)$$

Knowing the above discrepancy bound, we are now ready to ask about the size of the polynomial lattice point set required to achieve a weighted star discrepancy not exceeding some  $\varepsilon$  threshold. In particular, we would like to know how this size depends on the dimension  $s$  and on  $\varepsilon$ .

**Corollary 2** *Let  $N = p^m$ ,  $\gamma$  and  $\mathbf{w}$  as in Theorem 1 and consider the problem of constructing generating vectors for polynomial lattice point sets with small weighted star discrepancy. Then*

$$\sum_{j=1}^{\infty} \gamma_j p^{w_j} < \infty$$

*is a sufficient condition for strong polynomial tractability. This condition further implies  $D_{N, \gamma}^*((x^{w_1}g_1, \dots, x^{w_s}g_s), x^m) = \mathcal{O}(N^{-1+\delta})$ , with the implied constant independent of  $s$ , for any  $\delta > 0$ , where  $(g_1, \dots, g_s) \in \mathcal{G}_{p, m-\mathbf{w}}^s(x^m)$  is constructed using Algorithm 1.*

*Proof.* Construct a generating vector  $(g_1, \dots, g_s) \in \mathcal{G}_{p, m-\mathbf{w}}^s(x^m)$  applying Algorithm 1 and consider its weighted star discrepancy, bounded by (5). Following closely the lines of the argumentation in [7, Section 5] and noticing that  $2m \frac{p^2-1}{3p} = \mathcal{O}(\log N)$  we obtain the result. More precisely, provided that the  $\gamma_j p^{w_j}$ 's are summable, we have a means to construct polynomial lattice point sets  $\mathcal{P}(\mathbf{g}, f)$  with  $D_{N, \gamma}^*(\mathbf{g}, f) \leq \varepsilon$ , whose sizes grow polynomially in  $\varepsilon^{-1}$  and are independent of the dimension. As a result the problem is strongly polynomially tractable. The discrepancy result  $D_{N, \gamma}^*((x^{w_1}g_1, \dots, x^{w_s}g_s), x^m) = \mathcal{O}(N^{-1+\delta})$  also follows directly from [7].  $\square$

**Remark 2** Recall that  $t = \max\{j \in \mathbb{N} : w_j < m\}$  and note that setting  $w_j = m$  for all  $j > t$  does neither change the bound on the weighted star discrepancy nor the computational cost of Algorithm 1. It might change the generating vector though. If so, however, only components with very little influence on the quality of the point set are altered. Defining  $w_j = m$  for all  $j > t$ , it suffices to have a summable weight sequence  $\gamma$  in order to achieve strong polynomial tractability, as long as  $t$  is finite.

In order to show Theorem 1 we need several auxiliary results.

**Lemma 1** Let  $a \in \mathbb{F}_p[x]$  be monic. Then we have

$$\sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ a|h}} r_p(h) = (m - \deg(a)) \frac{p^2 - 1}{3p} p^{-\deg(a)}.$$

In particular, for  $a = 1$  this formula yields

$$\sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) = m \frac{p^2 - 1}{3p}.$$

*Proof.* This fact follows from [1, p. 1055] (by setting  $\gamma_{d+1} = 1$ ). The special case  $a = 1$  also follows from [4, Lemma 2.2] by setting  $s = 1$ .  $\square$

For our purposes, it is convenient to write  $R_\gamma^s(\mathbf{g}, f)$  from (4) in an alternative way. To this end, we introduce some notation. For a Laurent series  $L \in \mathbb{F}_p((x^{-1}))$  we denote by  $c_{-1}(L)$  its coefficient of  $x^{-1}$ , i.e., its residuum. Further, we set  $X_p(L) := \chi_p(c_{-1}(L))$ , where  $\chi_p$  is a non-trivial additive character of  $\mathbb{F}_p$ . One could for instance choose  $\chi_p(n) = e^{\frac{2\pi i}{p}n}$  for  $n \in \mathbb{F}_p$  (see, e.g., [11]). It is clear that  $X_p(L) = 1$  if  $L$  is a polynomial and that  $X_p(L_1 + L_2) = X_p(L_1)X_p(L_2)$  for  $L_1, L_2 \in \mathbb{F}_p((x^{-1}))$ . From [12, p. 78] we know that

$$\sum_{v \in G_{p,m}} X_p\left(\frac{v}{f}g\right) = \begin{cases} p^m & \text{if } f \mid g, \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

**Lemma 2** We have

$$R_\gamma^s(\mathbf{g}, f) = - \prod_{i=1}^s (1 + \gamma_i) + \frac{1}{p^m} \sum_{v \in G_{p,m}} \prod_{i=1}^s \left( 1 + \gamma_i + \gamma_i \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p\left(\frac{v}{f} h g_i\right) \right).$$

*Proof.* We employ the properties of  $X_p$  as stated above to obtain from (4)

$$\begin{aligned} R_\gamma^s(\mathbf{g}, f) &= - \prod_{i=1}^s (1 + \gamma_i) + \frac{1}{p^m} \sum_{\mathbf{h} \in G_{p,m}^s} \left( \prod_{i=1}^s r_p(h_i, \gamma_i) \right) \sum_{v \in G_{p,m}} X_p\left(\frac{v}{f} \mathbf{h} \cdot \mathbf{g}\right) \\ &= - \prod_{i=1}^s (1 + \gamma_i) + \frac{1}{p^m} \sum_{v \in G_{p,m}} \prod_{i=1}^s \left( \sum_{h_i \in G_{p,m}} r_p(h_i, \gamma_i) X_p\left(\frac{v}{f} h_i g_i\right) \right) \\ &= - \prod_{i=1}^s (1 + \gamma_i) + \frac{1}{p^m} \sum_{v \in G_{p,m}} \prod_{i=1}^s \left( 1 + \gamma_i + \gamma_i \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p\left(\frac{v}{f} h g_i\right) \right), \end{aligned}$$

and the claimed formula is verified.  $\square$



Now we study a sum which will appear later in the proof of Theorem 1 and show an upper bound for it.

**Lemma 3** *Let  $w \in \mathbb{N}_0$  and  $v \in G_{p,m}$ . Let*

$$Y_{p^m,w}(v, x^m) := \sum_{g \in \mathcal{G}_{p,m-w}(x^m)} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^w g \right),$$

where  $x^w$  denotes the polynomial  $f(x) = x^w$ . Then we have

$$\frac{1}{\#\mathcal{G}_{p,m-w}(x^m)} \sum_{v \in G_{p,m}} |Y_{p^m,w}(v, x^m)| \leq 2p^{\min\{w,m\}} m \frac{p^2 - 1}{3p}.$$

*Proof.* Let us first assume that  $w \geq m$ . Then we have  $\mathcal{G}_{p,m-w}(x^m) = \{1\}$  and therefore

$$Y_{p^m,w}(v, x^m) = \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p(v h x^{w-m}) = \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) = m \frac{p^2 - 1}{3p}$$

with Lemma 1. This leads to

$$\frac{1}{\#\mathcal{G}_{p,m-w}(x^m)} \sum_{v \in G_{p,m}} |Y_{p^m,w}(v, x^m)| = p^m m \frac{p^2 - 1}{3p} \leq 2p^{\min\{w,m\}} m \frac{p^2 - 1}{3p}$$

in this case. For the rest of the proof let  $w < m$  and additionally we abbreviate  $\#\mathcal{G}_{p,m-w}(x^m)$  by  $\#\mathcal{G}$ . We write

$$\frac{1}{\#\mathcal{G}} \sum_{v \in G_{p,m}} |Y_{p^m,w}(v, x^m)| = \frac{1}{\#\mathcal{G}} \sum_{\substack{v \in G_{p,m} \\ x^{m-w} | v}} |Y_{p^m,w}(v, x^m)| + \frac{1}{\#\mathcal{G}} \sum_{\substack{v \in G_{p,m} \\ x^{m-w} \nmid v}} |Y_{p^m,w}(v, x^m)|.$$

In what follows, we refer to the latter sums as

$$S_1 := \frac{1}{\#\mathcal{G}} \sum_{\substack{v \in G_{p,m} \\ x^{m-w} | v}} |Y_{p^m,w}(v, x^m)| \quad \text{and} \quad S_2 := \frac{1}{\#\mathcal{G}} \sum_{\substack{v \in G_{p,m} \\ x^{m-w} \nmid v}} |Y_{p^m,w}(v, x^m)|.$$

We may uniquely write any  $v \in G_{p,m} \setminus \{0\}$  in the form  $v = qx^{m-w} + \ell$ , where  $q, \ell \in \mathbb{F}_q[x]$  with  $\deg(q) < w$  and  $\deg(\ell) < m - w$ . Using the properties of  $X_p$  it is clear that  $Y_{p^m,w}(v, x^m) = Y_{p^m,w}(\ell, x^m)$  and hence

$$\begin{aligned} S_1 &= \frac{1}{\#\mathcal{G}} \sum_{\substack{v \in G_{p,m} \\ x^{m-w} | v}} |Y_{p^m,w}(0, x^m)| = \sum_{\substack{v \in G_{p,m} \\ x^{m-w} | v}} \frac{1}{\#\mathcal{G}} \sum_{g \in \mathcal{G}_{p,m-w}(x^m)} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \\ &= \sum_{\substack{v \in G_{p,m} \\ x^{m-w} | v}} m \frac{p^2 - 1}{3p} = p^{\min\{w,m\}} m \frac{p^2 - 1}{3p}. \end{aligned}$$

We move on to  $S_2$ . Let  $e(\ell) := \max\{k \in \{0, 1, \dots, m - w - 1\} : x^k \mid \ell\}$ . With this definition we may display  $S_2$  as

$$S_2 = \frac{p^w}{\#\mathcal{G}} \sum_{k=0}^{m-w-1} \sum_{\substack{\ell \in G_{p,m-w} \setminus \{0\} \\ e(\ell)=k}} |Y_{p^m,w}(\ell, x^m)|. \quad (7)$$

In the following, we compute  $Y_{p^m,w}(\ell, x^m)$  for  $\ell \in G_{p,m-w} \setminus \{0\}$  with  $e(\ell) = k$ . Let  $\mu_p$  be the Möbius function on the set of monic polynomials over  $\mathbb{F}_p$ , i.e.,  $\mu_p : \mathbb{F}_p[x] \rightarrow \{-1, 0, 1\}$  and

$$\mu_p(h) = \begin{cases} (-1)^\nu & \text{if } h \text{ is squarefree and has } \nu \text{ irreducible factors,} \\ 0 & \text{else.} \end{cases}$$

The fact that  $\mu_p(1) = 1$ ,  $\mu_p(x) = -1$  and  $\mu_p(x^i) = 0$  for  $i \in \mathbb{N}$ ,  $i \geq 2$ , yields the equivalence of  $\sum_{t|\gcd(x^{m-w}, g)} \mu_p(t) = 1$  and  $\gcd(x^{m-w}, g) = 1$ . Therefore we can write

$$\begin{aligned} Y_{p^m,w}(\ell, x^m) &= \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \sum_{g \in G_{p,m-w}} X_p\left(\frac{\ell}{x^{m-w}}hg\right) \sum_{t|\gcd(x^{m-w}, g)} \mu_p(t) \\ &= \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \sum_{t|x^{m-w}} \mu_p(t) \sum_{\substack{g \in G_{p,m-w} \\ t|g}} X_p\left(\frac{\ell}{x^{m-w}}hg\right) \\ &= \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \sum_{t|x^{m-w}} \mu_p(t) \sum_{a \in G_{p,m-w-\deg(t)}} X_p\left(\frac{\ell}{x^{m-w}}hat\right) \\ &= \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) \sum_{a \in G_{p,\deg(t)}} X_p\left(\frac{a}{t}h\ell\right) \\ &= \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \sum_{\substack{t|x^{m-w} \\ t|h\ell}} \mu_p\left(\frac{x^{m-w}}{t}\right) p^{\deg(t)} \\ &= \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) p^{\deg(t)} \sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ t|h\ell}} r_p(h). \end{aligned}$$

The equivalence of the conditions  $t \mid h\ell$  and  $\frac{t}{\gcd(t,\ell)} \mid h$  yields

$$Y_{p^m,w}(\ell, x^m) = \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) p^{\deg(t)} \sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ \frac{t}{\gcd(t,\ell)}|h}} r_p(h).$$

We investigate the inner sum and use Lemma 1 with  $a = \frac{t}{\gcd(t,\ell)}$  to find

$$\sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ \frac{t}{\gcd(t,\ell)}|h}} r_p(h) = \left(m - \deg\left(\frac{t}{\gcd(t,\ell)}\right)\right) \frac{p^2 - 1}{3p} p^{-\deg\left(\frac{t}{\gcd(t,\ell)}\right)}.$$

Now we have

$$\begin{aligned} Y_{p^m,w}(\ell, x^m) &= \frac{p^2 - 1}{3p} \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) \left(m - \deg\left(\frac{t}{\gcd(t,\ell)}\right)\right) p^{\deg(\gcd(t,\ell))} \\ &= \frac{p^2 - 1}{3p} m \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) p^{\deg(\gcd(t,\ell))} \\ &\quad - \frac{p^2 - 1}{3p} \sum_{t|x^{m-w}} \mu_p\left(\frac{x^{m-w}}{t}\right) \deg\left(\frac{t}{\gcd(t,\ell)}\right) p^{\deg(\gcd(t,\ell))}. \end{aligned}$$

From the fact that  $e(\ell) = k \leq m - w - 1$  we obtain  $\gcd(x^{m-w}, \ell) = \gcd(x^{m-w-1}, \ell) = x^k$ . This observation leads to

$$\sum_{t|x^{m-w}} \mu_p \left( \frac{x^{m-w}}{t} \right) p^{\deg(\gcd(t, \ell))} = p^{\deg(\gcd(x^{m-w}, \ell))} - p^{\deg(\gcd(x^{m-w-1}, \ell))} = 0$$

and

$$\begin{aligned} & \sum_{t|x^{m-w}} \mu_p \left( \frac{x^{m-w}}{t} \right) \deg \left( \frac{t}{\gcd(t, \ell)} \right) p^{\deg(\gcd(t, \ell))} \\ &= \deg \left( \frac{x^{m-w}}{\gcd(x^{m-w}, \ell)} \right) p^{\deg(\gcd(x^{m-w}, \ell))} - \deg \left( \frac{x^{m-w-1}}{\gcd(x^{m-w-1}, \ell)} \right) p^{\deg(\gcd(x^{m-w-1}, \ell))} \\ &= (m - w - k)p^k - (m - w - k - 1)p^k = p^k. \end{aligned}$$

Altogether we have

$$Y_{p^m, w}(\ell, x^m) = -\frac{p^2 - 1}{3p} p^k.$$

Inserting this result into (7) yields

$$S_2 = \frac{p^w}{\#\mathcal{G}} \frac{p^2 - 1}{3p} \sum_{k=0}^{m-w-1} p^k \sum_{\substack{\ell \in G_{p, m-w} \setminus \{0\} \\ e(\ell)=k}} 1.$$

Since

$$\begin{aligned} & \#\{\ell \in G_{p, m-w} \setminus \{0\} : e(\ell) = k\} \\ &= \#\{\ell \in G_{p, m-w} \setminus \{0\} : x^k \mid \ell\} - \#\{\ell \in G_{p, m-w} \setminus \{0\} : x^{k+1} \mid \ell\} \\ &= p^{m-w-k} - 1 - (p^{m-w-k-1} - 1) = p^{m-w-k-1}(p - 1), \end{aligned}$$

we have

$$\begin{aligned} S_2 &= \frac{p^w}{p^{m-w-1}(p-1)} \frac{p^2 - 1}{3p} \sum_{k=0}^{m-w-1} p^k p^{m-w-k-1}(p-1) \\ &= p^w \frac{p^2 - 1}{3p} (m - w) \leq p^{\min\{w, m\}} m \frac{p^2 - 1}{3p}. \end{aligned}$$

Summarizing, we have shown

$$\frac{1}{\#\mathcal{G}} \sum_{v \in G_{p, m}} |Y_{p^m, w}(v, x^m)| = S_1 + S_2 \leq 2p^{\min\{w, m\}} m \frac{p^2 - 1}{3p},$$

which completes the proof. □

Now we are ready to prove Theorem 1 using induction on  $d$ .

*Proof.* We show the result for  $d = 1$ . From Lemma 2 we have

$$R_{\gamma}^1((x^{w_1}), x^m) = -(1 + \gamma_1) + \frac{1}{p^m} \sum_{v \in G_{p, m}} \left( 1 + \gamma_1 + \gamma_1 \sum_{h \in G_{p, m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_1} \right) \right)$$

$$= \frac{\gamma_1}{p^m} \sum_{v \in G_{p,m}} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_1} \right).$$

If  $w_1 \geq m$ , then

$$\begin{aligned} R_\gamma^1((x^{w_1}), x^m) &= \frac{\gamma_1}{p^m} \sum_{v \in G_{p,m}} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) = \frac{\gamma_1}{p^m} p^{\min\{w_1, m\}} m \frac{p^2 - 1}{3p} \\ &\leq \frac{1}{p^m} \left( 1 + \gamma_1 + \gamma_1 2p^{\min\{w_1, m\}} m \frac{p^2 - 1}{3p} \right). \end{aligned}$$

If  $w_1 < m$ , then we can write

$$\begin{aligned} R_\gamma^1((x^{w_1}), x^m) &= \frac{\gamma_1}{p^m} \sum_{v \in G_{p,m}} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_1} \right) \\ &= \frac{\gamma_1}{p^m} \sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ x^{m-w_1} | h}} r_p(h) \sum_{v \in G_{p,m}} X_p \left( \frac{v}{x^m} h x^{w_1} \right) \\ &\quad + \frac{\gamma_1}{p^m} \sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ x^{m-w_1} \nmid h}} r_p(h) \sum_{v \in G_{p,m}} X_p \left( \frac{v}{x^m} h x^{w_1} \right) \\ &= \gamma_1 \sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ x^{m-w_1} | h}} r_p(h), \end{aligned}$$

where we used (6) in the latter step. We regard Lemma 1 with  $a = x^{m-w_1}$  to compute

$$\sum_{\substack{h \in G_{p,m} \setminus \{0\} \\ x^{m-w_1} | h}} r_p(h) = \frac{1}{p^m} p^{w_1} w_1 \frac{p^2 - 1}{3p} \leq \frac{1}{p^m} p^{\min\{w_1, m\}} m \frac{p^2 - 1}{3p},$$

which leads to the desired result also in this case.

Now let  $d \in [s-1]$ . Assume that we have some  $(g_1, \dots, g_d) \in \mathcal{G}_{p,m-w}^d(x^m)$  such that

$$R_\gamma^d((x^{w_1} g_1, \dots, x^{w_d} g_d), x^m) \leq \frac{1}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right).$$

Let  $g^* \in \mathcal{G}_{p,m-w_{d+1}}(x^m)$  be such that  $R_\gamma^{d+1}((x^{w_1} g_1, \dots, x^{w_d} g_d, x^{w_{d+1}} g_{d+1}), x^m)$  is minimized as a function of  $g_{d+1}$  for  $g_{d+1} = g^*$ . Then we have

$$\begin{aligned} R_\gamma^{d+1}((x^{w_1} g_1, \dots, x^{w_d} g_d, x^{w_{d+1}} g^*), x^m) &= -(1 + \gamma_{d+1}) \prod_{i=1}^d (1 + \gamma_i) \\ &\quad + \frac{1}{p^m} \sum_{v \in G_{p,m}} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_i} g_i \right) \right) \\ &\quad \times \left( 1 + \gamma_{d+1} + \gamma_{d+1} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_{d+1}} g^* \right) \right) \\ &= (1 + \gamma_{d+1}) R_\gamma^d((x^{w_1} g_1, \dots, x^{w_d} g_d), x^m) + L(g^*), \end{aligned} \tag{8}$$

where

$$L(g^*) = \frac{\gamma_{d+1}}{p^m} \sum_{v \in G_{p,m}} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_{d+1}} g^* \right) \\ \times \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_i} g_i \right) \right).$$

A minimizer  $g^*$  of  $R_\gamma^{d+1}((x^{w_1}g_1, \dots, x^{w_d}g_d, x^{w_{d+1}}g_{d+1}), x^m)$  is also a minimizer of  $L(g_{d+1})$ . Combining (4) and (8) we obtain that  $R_\gamma^d(\mathbf{g}, f) \in \mathbb{R}$  for all  $d \in [s]$ . Moreover with equation (10), established later on in Section 2.2, and the fact that  $r_p(h, \gamma) > 0$  for all  $h \in G_{p,m}$  and  $\gamma \in (0, 1]$ , we get that  $L(g) \in \mathbb{R}^+$  for all  $g \in \mathcal{G}_{p,m-w_{d+1}}(x^m)$ . Thus we may bound  $L(g^*)$  by the mean over all  $g \in \mathcal{G}_{p,m-w_{d+1}}(x^m)$ , hence

$$L(g^*) \leq \frac{1}{\#\mathcal{G}_{p,m-w_{d+1}}(x^m)} \sum_{g_{d+1} \in \mathcal{G}_{p,m-w_{d+1}}(x^m)} L(g_{d+1}) \\ \leq \frac{\gamma_{d+1}}{p^m} \sum_{v \in G_{p,m}} \frac{1}{\#\mathcal{G}_{p,m-w_{d+1}}(x^m)} \\ \times \left| \sum_{g_{d+1} \in \mathcal{G}_{p,m-w_{d+1}}(x^m)} \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) X_p \left( \frac{v}{x^m} h x^{w_{d+1}} g_{d+1} \right) \right| \\ \times \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i \sum_{h \in G_{p,m} \setminus \{0\}} r_p(h) \left| X_p \left( \frac{v}{x^m} h x^{w_i} g_i \right) \right| \right) \\ \leq \frac{\gamma_{d+1}}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i m \frac{p^2 - 1}{3p} \right) \sum_{v \in G_{p,m}} \frac{|Y_{p^m, w_{d+1}}(v, x^m)|}{\#\mathcal{G}_{p,m-w_{d+1}}(x^m)},$$

where we used the estimate  $\left| X_p \left( \frac{v}{x^m} h x^{w_i} g_i \right) \right| \leq 1$  in the last step. With the induction hypothesis and Lemma 3 this leads to

$$R_\gamma^{d+1}((x^{w_1}g_1, \dots, x^{w_d}g_d, x^{w_{d+1}}g^*), x^m) \\ \leq (1 + \gamma_{d+1}) \frac{1}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right) \\ + \frac{\gamma_{d+1}}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i m \frac{p^2 - 1}{3p} \right) 2p^{\min\{w_{d+1}, m\}} m \frac{p^2 - 1}{3p} \\ \leq \frac{1}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right) \left( 1 + \gamma_{d+1} + \gamma_{d+1} 2p^{\min\{w_{d+1}, m\}} m \frac{p^2 - 1}{3p} \right) \\ = \frac{1}{p^m} \prod_{i=1}^{d+1} \left( 1 + \gamma_i + \gamma_i 2p^{\min\{w_i, m\}} m \frac{p^2 - 1}{3p} \right).$$

□

### The reduced fast CBC construction

So far we have seen how to construct a generating vector  $\mathbf{g}$  of the point set  $\mathcal{P}(\mathbf{g}, x^m)$ . In fact Algorithm 1 can be made much faster using results of [2, 18, 17]. In this section we are investigating and improving Algorithm 1 and additionally analyzing the computational cost of the improved algorithm.

As explained in the following lines Walsh functions are a suitable tool for analyzing the computational cost of CBC algorithms for constructing polynomial lattice point sets. Let  $\omega = e^{2\pi i/p}$ ,  $x \in [0, 1)$  and  $h$  a nonnegative integer with base  $p$  representation  $x = x_1/p + x_2/p^2 + \dots$  and  $h = h_0 + h_1p + \dots + h_rp^r$ , respectively. Then we define

$$\text{wal}_h : [0, 1) \rightarrow \mathbb{C}, \text{wal}_h(x) := \omega^{h_0x_1 + \dots + h_rx_{r+1}}.$$

The Walsh function system  $\{\text{wal}_h \mid h = 0, 1, \dots\}$  is a complete orthonormal basis in  $L_2([0, 1))$  which has been used in the analysis of the discrepancy of digital nets (an important class of low-discrepancy point sets which contains polynomial lattice point sets) several times before, see for example [4, 6, 8]. For further information on Walsh functions see [5, Appendix A].

Let  $d \geq 1$ ,  $N = p^m$ . For  $P(\mathbf{g}, f) = \{\mathbf{x}_0, \dots, \mathbf{x}_{p^m-1}\}$  with  $\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)})$  we have the formula (see [4, Section 4])

$$\frac{1}{p^m} \sum_{n=0}^{p^m-1} \prod_{i=1}^s \text{wal}_{h_i}(x_n^{(i)}) = \begin{cases} 1 & \text{if } \mathbf{g} \cdot \mathbf{h} \equiv 0 \pmod{f}, \\ 0 & \text{otherwise,} \end{cases}$$

which allows us to rewrite  $R_\gamma^d(\mathbf{g}, x^m)$  in the following way

$$R_\gamma^d(\mathbf{g}, x^m) = - \prod_{i=1}^d (1 + \gamma_i) + \frac{1}{p^m} \sum_{n=0}^{p^m-1} \prod_{i=1}^d \sum_{h=0}^{p^m-1} r_p(h, \gamma_i) \text{wal}_h \left( \phi_m \left( \frac{nx^{w_i}g_i}{x^m} \right) \right).$$

Note that  $r_p(h, \gamma)$  is defined as in (4) and we identify the integer in base  $p$  representation  $h = h_0 + h_1p + \dots + h_rp^r$  with the polynomial  $h(x) = h_0 + h_1x + \dots + h_rx^r$ . If we set  $\psi\left(\frac{nx^{w_i}g_i}{x^m}\right) := \sum_{h=1}^{p^m-1} r_p(h) \text{wal}_h\left(\phi_m\left(\frac{nx^{w_i}g_i}{x^m}\right)\right)$  we get that

$$\begin{aligned} R_\gamma^d(\mathbf{g}, x^m) &= - \prod_{i=1}^d (1 + \gamma_i) + \frac{1}{p^m} \sum_{n=0}^{p^m-1} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i \psi \left( \frac{nx^{w_i}g_i}{x^m} \right) \right) \\ &= - \prod_{i=1}^d (1 + \gamma_i) + \frac{1}{p^m} \sum_{n=0}^{p^m-1} \eta_d(n), \end{aligned} \tag{9}$$

where  $\eta_d(n) = \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i \psi \left( \frac{nx^{w_i}g_i}{x^m} \right) \right)$ .

In [4, Section 4] it is proved that we can compute the at most  $N$  different values of  $\psi\left(\frac{r}{x^m}\right)$  for  $r \in G_{p,m}$  in  $\mathcal{O}(N)$  operations.

Let us now analyze one step of the reduced CBC Algorithm 1. Assuming we already have found  $(g_1, \dots, g_d) \in \mathcal{G}_{p,m-\mathbf{w}}^d(x^m)$  we have to minimize

$$R_\gamma^{d+1}((x^{w_1}g_1, \dots, x^{w_{d+1}}g_{d+1}), x^m)$$

as a function of  $g_{d+1} \in \mathcal{G}_{p,m-w_{d+1}}(x^m)$ . If  $w_{d+1} \geq m$  then  $g_{d+1} = 1$  and we are done. Let now  $w_{d+1} < m$ . From (9) we have that

$$\begin{aligned} R_\gamma^{d+1}((x^{w_1}g_1, \dots, x^{w_{d+1}}g_{d+1}), x^m) &= - \prod_{i=1}^{d+1} (1 + \gamma_i) + \frac{1}{p^m} \sum_{n=0}^{p^m-1} \eta_{d+1}(n) \\ &= - \prod_{i=1}^{d+1} (1 + \gamma_i) + \frac{1}{p^m} \sum_{n=0}^{p^m-1} \left( 1 + \gamma_{d+1} + \right. \end{aligned}$$

$$\gamma_{d+1} \psi \left( \frac{nx^{w_{d+1}}g_{d+1}}{x^m} \right) \eta_d(n) \Bigg).$$

In order to minimize  $R_\gamma^{d+1}((x^{w_1}g_1, \dots, x^{w_{d+1}}g_{d+1}), x^m)$  it is enough to minimize  $T_d(g) := \sum_{n=0}^{p^m-1} \psi(\frac{nx^{w_{d+1}}g}{x^m}) \eta_d(n)$ . As in [2, Section 4] we can represent this quantity using some specific  $(p^{m-w_{d+1}-1}(p-1) \times N)$ -matrix  $A$  and exploiting its additional structure. Let therefore

$$A = \left( \psi \left( \frac{nx^{w_{d+1}}g}{x^m} \right) \right)_{\substack{n \in \{0, \dots, N-1\}, \\ g \in G_{p, m-w_{d+1}}(x^m)}} \text{ and } \boldsymbol{\eta}_d = (\eta_d(0), \dots, \eta_d(N-1))^\top.$$

First of all observe that we get  $(T(g))_{g \in G_{p, m-w_{d+1}}(x^m)} = A\boldsymbol{\eta}_d$ . Secondly the matrix  $A$  is a block matrix and can be written in the following form

$$A = \left( \Omega^{(m-w_{d+1})} \dots \Omega^{(m-w_{d+1})} \right), \text{ where } \Omega^{(l)} = \left( \psi \left( \frac{nx^{w_{d+1}}g}{x^m} \right) \right)_{\substack{n \in \{0, \dots, p^l-1\} \\ g \in G_{p, m-w_{d+1}}(x^m)}}.$$

If  $\mathbf{x}$  is any vector of size  $p^m$  then we compute

$$A\mathbf{x} = \Omega^{(m-w_{d+1})}\mathbf{x}_1 + \dots + \Omega^{(m-w_{d+1})}\mathbf{x}_{b^{w_d}} = \Omega^{(m-w_{d+1})}(\mathbf{x}_1 + \dots + \mathbf{x}_{b^{w_d}}).$$

With this representation we can apply the machinery of [17, 18] and get that multiplication with  $\Omega^{(m-w_{d+1})}$  can be done in  $\mathcal{O}((m-w_{d+1})p^{m-w_{d+1}})$  operations. Summarizing we have:

## Algorithm 2

1. Compute  $\psi(\frac{r}{x^m})$  for  $r \in G_{p, m}$ .
2. Set  $\eta_1(n) = \psi(\frac{nx^{w_1}g_1}{x^m})$  for  $n = 0, \dots, p^m - 1$ .
3. Set  $g_1 = 1$ ,  $d = 2$  and  $t = \max\{j \in [s] \mid w_j < m\}$ .  
While  $d \leq \min\{s, t\}$ ,
  - (a) Partition  $\eta_{d-1}$  into  $p^{w_d}$  vectors  $\eta_{d-1}^{(1)}, \dots, \eta_{d-1}^{(p^{w_d})}$  of length  $p^{m-w_d}$  and let  $\eta' = \sum_{i=1}^{p^{w_d}} \eta_{d-1}^{(i)}$ .
  - (b) Let  $T_d(g) = \Omega^{(m-w_d)}\eta'$ .
  - (c) Let  $g_d = \arg\min_g T_d(g)$ .
  - (d) Let  $\eta_d(n) = \eta_{d-1}(n)\psi(\frac{nx^{w_d}g_d}{x^m})$ .
  - (e) Increase  $d$  by 1.
4. If  $s \geq t$  then set  $g_t = g_{t+1} \dots = g_s = 1$ .

Similar to [2] we obtain from the observations in this section the following theorem:

**Theorem 2** *The cost of Algorithm 2 is*

$$\mathcal{O} \left( p^m + \min\{s, t\}p^m + \sum_{d=1}^{\min\{s, t\}} (m - w_d)p^{m-w_d} \right).$$

## 2.2 Polynomial lattice point sets for irreducible $f$

Finally we want to consider the special case where  $f$  is an irreducible polynomial. So, for this section let  $f$  be an irreducible polynomial over  $\mathbb{F}_p$  with  $\deg(f) = m$ .

**Theorem 3** *Let  $\gamma$  and  $\mathbf{w}$  as in Theorem 1 and let  $f \in \mathbb{F}_p[x]$  be an irreducible polynomial with  $\deg(f) = m$ . Let further  $(g_1, \dots, g_s) \in \mathcal{G}_{p,m-\mathbf{w}}^s(f)$  be constructed according to Algorithm 1. Then we have for every  $d \in [s]$*

$$R_\gamma^d((x^{w_1}g_1, \dots, x^{w_d}g_d), f) \leq \frac{1}{p^m} \prod_{i=1}^d \left(1 + \gamma_i + \gamma_i p^{\min\{w_i, m\}} m \frac{p+1}{3}\right).$$

*Proof.* We will prove this result by induction on  $d$ . According to Algorithm 1 we know that  $g_1 = 1$  for  $d = 1$ . Therefore  $R_\gamma^1((x^{w_1}g_1), f) = 0$  since for all  $h \in G_{p,m}$  we have  $\deg(h) < m$  and hence the congruence  $hx^{w_1} \equiv 0 \pmod{f}$  has no solutions.

Let  $d \in [s-1]$  and assume that we have already found  $(g_1, \dots, g_d) \in \mathcal{G}_{p,m-\mathbf{w}}^d(f)$ . For  $\mathbf{g} = (x^{w_1}g_1, \dots, x^{w_d}g_d)$  we have from (4) that

$$R_\gamma^{d+1}((\mathbf{g}, x^{w_{d+1}}g_{d+1}), f) = (1 + \gamma_{d+1})R_\gamma^d(\mathbf{g}, f) + \theta(g_{d+1}), \quad (10)$$

where we proceeded similarly as in the proof of Theorem 1. Here we have

$$\theta(g_{d+1}) = \sum_{h_{d+1} \in G_{p,m} \setminus \{0\}} r_p(h_{d+1}, \gamma_{d+1}) \sum_{\substack{\mathbf{h} \in G_{p,m}^d \\ \mathbf{h} \cdot \mathbf{g} \equiv -h_{d+1}x^{w_{d+1}}g_{d+1} \pmod{f}}} \prod_{i=1}^d r_p(h_i, \gamma_i).$$

Let  $g^* \in \mathcal{G}_{p,m-w_{d+1}}(f)$  be a minimizer of  $R_\gamma^{d+1}((\mathbf{g}, x^{w_{d+1}}g_{d+1}), f)$  as a function of  $g_{d+1}$ . Therefore  $g^*$  also minimizes  $\theta(g_{d+1})$ . Bounding  $\theta(g^*)$  by its mean we obtain

$$\begin{aligned} \theta(g^*) &\leq \frac{1}{\#\mathcal{G}_{p,m-w_{d+1}}(f)} \sum_{h_{d+1} \in G_{p,m} \setminus \{0\}} r_p(h_{d+1}, \gamma_{d+1}) \\ &\quad \times \sum_{\mathbf{h} \in G_{p,m}^d} \left( \prod_{i=1}^d r_p(h_i, \gamma_i) \right) \sum_{\substack{g_{d+1} \in \mathcal{G}_{p,m-w_{d+1}}(f) \\ \mathbf{h} \cdot \mathbf{g} \equiv -h_{d+1}x^{w_{d+1}}g_{d+1} \pmod{f}}} 1. \end{aligned}$$

Observe that  $\gcd(f, h_{d+1}x^{w_{d+1}}) = 1$ . Therefore the congruence  $h_{d+1}x^{w_{d+1}}g_{d+1} \equiv -\mathbf{h} \cdot \mathbf{g} \pmod{f}$  has a unique solution in  $G_{p,m}$  but not necessarily in  $\mathcal{G}_{p,m-w_{d+1}}(f)$ . In the case that  $-\mathbf{h} \cdot \mathbf{g} \not\equiv 0 \pmod{f}$  we conclude that the congruence has at most one solution in  $\mathcal{G}_{p,m-w_{d+1}}(f)$ . If  $-\mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod{f}$  the congruence has no solution in  $\mathcal{G}_{p,m-w_{d+1}}(f)$  since  $0 \notin \mathcal{G}_{p,m-w_{d+1}}(f)$ . Hence we find by an application of [4, Lemma 3.3]

$$\begin{aligned} \theta(g^*) &\leq \frac{1}{\#\mathcal{G}_{p,m-w_{d+1}}(f)} \sum_{h_{d+1} \in G_{p,m} \setminus \{0\}} r_p(h_{d+1}, \gamma_{d+1}) \sum_{\mathbf{h} \in G_{p,m}^d} \prod_{i=1}^d r_p(h_i, \gamma_i) \\ &= \frac{1}{\#\mathcal{G}_{p,m-w_{d+1}}(f)} \left[ \prod_{i=1}^d \left(1 + \gamma_i + \gamma_i m \frac{p^2-1}{3p}\right) \right] \left( \gamma_{d+1} m \frac{p^2-1}{3p} \right). \end{aligned}$$



By (10) and the induction hypothesis we have that

$$\begin{aligned}
R_\gamma^{d+1}((\mathbf{g}, x^{w_{d+1}} g_{d+1}), f) &= (1 + \gamma_{d+1}) R_\gamma^d(\mathbf{g}, f) + \theta(g_{d+1}) \\
&\leq \frac{1}{p^m} \prod_{i=1}^d \left( 1 + \gamma_i + \gamma_i p^{\min\{w_i, m\}} m^{\frac{p+1}{3}} \right) \\
&\quad \times \left( 1 + \gamma_{d+1} + \gamma_{d+1} \frac{p^m}{\#\mathcal{G}_{p, m-w_{d+1}}(f)} m^{\frac{p^2-1}{3p}} \right) \\
&\leq \frac{1}{p^m} \prod_{i=1}^{d+1} \left( 1 + \gamma_i + \gamma_i p^{\min\{w_i, m\}} m^{\frac{p+1}{3}} \right),
\end{aligned}$$

where we used in the latter step that  $\frac{p^m}{\#\mathcal{G}_{p, m-w_{d+1}}(f)} \leq \frac{p}{p-1} p^{\min\{w_{d+1}, m\}}$ . This follows from the fact that  $\#\mathcal{G}_{p, m-w_{d+1}}(f) = p^{m-w_{d+1}} - 1$  if  $w_{d+1} < m$  and  $\#\mathcal{G}_{p, m-w_{d+1}}(f) = 1$  if  $w_{d+1} \geq m$ . This finishes the proof of Theorem 3.  $\square$

As an immediate consequence of (3) and Theorem 3 we obtain the following result.

**Corollary 3** *Let  $N = p^m$ ,  $(w_j)_{j \geq 1}$  be a non-decreasing sequence of nonnegative integers and let  $(g_1, \dots, g_s) \in \mathcal{G}_{p, m-\mathbf{w}}^s(f)$  for irreducible  $f \in G_{p, m}$  be constructed using Algorithm 1. Then the polynomial lattice point set  $\mathcal{P}((x^{w_1} g_1, \dots, x^{w_s} g_s), f)$  has a weighted star discrepancy*

$$\begin{aligned}
D_{N, \gamma}^*((x^{w_1} g_1, \dots, x^{w_s} g_s), f) \\
\leq \sum_{\substack{\mathbf{u} \subseteq [s] \\ \mathbf{u} \neq \emptyset}} \gamma_{\mathbf{u}} \left( 1 - \left( 1 - \frac{1}{N} \right)^{|\mathbf{u}|} \right) + \frac{1}{N} \prod_{i=1}^s \left( 1 + \gamma_i + \gamma_i p^{\min\{w_i, m\}} m^{\frac{p+1}{3}} \right).
\end{aligned}$$

**Remark 3** *Using the same argumentation as in Corollary 2 we again obtain the sufficient condition  $\sum_{j=1}^{\infty} \gamma_j p^{w_j} < \infty$  for strong polynomial tractability and for the discrepancy bound  $D_{N, \gamma}^*((x^{w_1} g_1, \dots, x^{w_s} g_s), f) = \mathcal{O}(N^{-1+\delta})$ , with the implied constant independent of  $s$ , for any  $\delta > 0$ .*

**Acknowledgements.** We would like to thank Peter Kritzer and Friedrich Pillichshammer for their valuable comments and suggestions which helped to improve our paper.

## References

- [1] J. Dick, P. Kritzer, G. Leobacher, F. Pillichshammer, Constructions of general polynomial lattice rules based on the weighted star discrepancy, *Finite Fields Appl.* 13 (2007) 1045–1070.
- [2] J. Dick, P. Kritzer, G. Leobacher, F. Pillichshammer, A reduced fast component-by-component construction of lattice points for integration in weighted spaces with fast decreasing weights, *J. Comput. Appl. Math.* 276 (2015) 1–15.
- [3] J. Dick, F. Kuo, I. H. Sloan, High-dimensional integration: the quasi-Monte Carlo way, *Acta Numer.* 22 (2013) 133–288.

- [4] J. Dick, G. Leobacher, F. Pillichshammer, Construction algorithms for digital nets with low weighted star discrepancy, *SIAM J. Numer. Anal.* 43 (2005) 76–95.
- [5] J. Dick, F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press Cambridge, 2010.
- [6] P. Hellekalek, General discrepancy estimates: the Walsh function system, *Acta Arith.* 67 (1994) 209–218
- [7] R. Kritzing, H. Laimer, A reduced fast component-by-component construction of lattice point sets with small weighted star discrepancy, *Unif. Distrib. Theory.* 10 (2015) 21–47.
- [8] G. Larcher, F. Pillichshammer, Sums of distances to the nearest integer and the discrepancy of digital nets, *Acta Arith.* 106 (2003) 379–408.
- [9] G. Leobacher, F. Pillichshammer, *Introduction to Quasi-Monte Carlo Integration and Applications, Compact Textbooks in Mathematics*, Birkhäuser, Cham, 2014.
- [10] S. Joe, Construction of good rank-1 lattice rules based on the weighted star discrepancy, In: *Monte Carlo and Quasi-Monte Carlo Methods 2004* (H. Niederreiter and D. Talay, eds.), Springer, Berlin, 2006, pp. 181–196.
- [11] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, UK, 1986.
- [12] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. Number 63 in CBMS-NFS Series in Applied Mathematics, SIAM, Philadelphia, 1992.
- [13] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields, *Czechoslovak Math. J.* 42 (1992) 143–166.
- [14] E. Novak, H. Woźniakowski, *Tractability of Multivariate Problems Vol. 1: Linear Information*. EMS, Zürich, 2008.
- [15] E. Novak, H. Woźniakowski, *Tractability of Multivariate Problems Vol. 2: Standard Information for Functionals*. EMS, Zürich, 2010.
- [16] E. Novak, H. Woźniakowski, *Tractability of Multivariate Problems Vol. 3: Standard Information for Operators*. EMS, Zürich, 2012.
- [17] D. Nuyens, R. Cools, Fast algorithms for component-by-component constructions of rank-1 lattice rules in shift-invariant reproducing kernel Hilbert spaces, *Math. Comp.* 75 (2006) 903–920.
- [18] D. Nuyens, R. Cools, Fast component-by-component constructions of rank-1 lattice rules with a non-prime number of points, *J. Complexity* 22 (2006) 4–28.
- [19] F. Pillichshammer, Polynomial Lattice Point Sets, In: *Monte Carlo and Quasi-Monte Carlo Methods 2010* (L. Plaskota and H. Wozniakowski ,eds.), Springer Verlag, 2012, pp. 189–210.

- [20] I. H. Sloan, A. V. Reztsov, Component-by-component construction of good lattice rules, *Math. Comp.* 71, no. 237 (2002) 263–273.
- [21] I. H. Sloan, H. Woźniakowski, When are quasi-Monte Carlo algorithms efficient for high-dimensional integrals? *J. Complexity* 14 (1998) 1–33.

**Authors' Addresses:**

Ralph Kritzing, Mario Neumüller, Institut für Finanzmathematik und Angewandte Zahlentheorie, Johannes Kepler Universität Linz, Altenbergerstr. 69, 4040 Linz, Austria.  
Email: [ralph.kritzing@jku.at](mailto:ralph.kritzing@jku.at), [mario.neumueller@jku.at](mailto:mario.neumueller@jku.at)

Helene Laimer, Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria.  
Email: [helene.laimer@ricam.oeaw.ac.at](mailto:helene.laimer@ricam.oeaw.ac.at)